Quorum
Cyber

Threat Intelligence LummaC2 Stealware

TLP Status: CLEAR

☎ +44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft
Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	24/08/2023	Initial Report Draft
1.0	05/09/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
	dd/mm/yyyy	

LummaC2 Stealer Threat

Overview

LummaC2 is an information-stealing malware strain that targets Windows systems and is available as a Stealer-as-a-Service[1]. The malware collects various target system data, including:

- Operating system (OS) version
- Hardware ID
- CPU
- RAM.

LummaC2 also has the capabilities to exfiltrate files and extract data from specific applications, including sensitive information from cryptocurrency wallets and two-factor authentication extensions[2]. The malware utilises obfuscation and code randomisation techniques to evade detection within target environment, thus maintaining a significant level of stealth within associated operations.

LummaC2 is distributed through various methods, including illegal cracks, keygens, phishing campaigns, as well as via disguised software setup files[3]. The stealware has been detected as being utilised by threat actors in conjunction with additional malware variants, such as RedLine Stealer and Amadey Loader. As of the time of writing, LummaC2 malware is being sold by a threat actor operating under different aliases on underground forums.

The most notable current events involving LummaC2 include its distribution through a phishing campaign exploiting OpenAI's ChatGPT software and its involvement in spreading the SectopRAT payload through the Amadey Bot malware[4].

Impact

Successful compromise by stealware variants, such as LummaC2, will almost certainly result in the loss and compromise of significant quantities of target system data. Most significantly, the loss of sensitive company and client credentials to a threat actor involved in stealware operations will almost certainly have serious implications to the security and integrity of company systems, employees and customers.

If compromised credentials remain unactioned, there is a realistic possibility that they will be sold to a range of opportunistic threat actors and will subsequently be used to enhance the effectiveness of further attack campaigns. If victims have applied poor password hygiene (such as using identical passwords across multiple platforms and websites) a leak of one set of credentials can have a major knock-on effect with regards to a wide array of systems and potentially lead to further compromise.

Incident Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide effective protection against malware threats such as LummaC2 Stealer. EDRs can alert system users of potential breaches and prevent the malware process during early stages of an attempted attack, therefore limiting the scope of damage.

[1] Malware Analysis: LummaC2 Stealer - SOCRadar® Cyber Intelligence Inc.
[2] Cyble — LummaC2 Stealer: A Potent Threat to Crypto Users
[3] New Infostealer LummaC2 Being Distributed Disguised As Illegal Cracks - ASEC BLOG (ahnlab.com)
[4] Cyble — The Growing Threat of ChatGPT-Based Phishing Attacks

Affected Products

- Windows OS

Containment, Mitigations & Remediations

It is recommended that upon the detection of compromised credentials, clients act promptly and issue password changes to affected users. Additionally, if password changes cannot be implemented or the account is no longer in active use, it is strongly recommended that the account is added to the 'deny list' so that it cannot be targeted in spear phishing campaigns. Furthermore, the enforcement of multi-factor authentication (MFA) is strongly recommended, as this can prevent adverse system access, even when credentials are compromised.

Threat intelligence gathering has also revealed a lack of strong password security and the use of basic, easy-to-crack passwords by users across all industry sectors. It is thus strongly recommended that clients adhere to the National Cyber Security Centre (NCSC) guidance[5] of implanting a password policy in which passwords are to be composed of three unrelated words and the incorporation of uppercase and lowercase characters and symbols.

Additionally, the use of an effective and monitored EDR solution is advised. An effective EDR tool will increase detection of malicious attempts of executable stealware files on a system, thus alerting the user to potential credential leaks.

Finally, it is strongly recommended that employees receive training on how to detect markers of phishing emails and potentially malicious websites, as this is the main method of initial access for LummaC2. Regular in-house training will prove to be effective in reducing the potency of future LummaC2 campaigns.

Indicators of Compromise

LummaC2 Stealer File Hashes (SHA-256):

- 89014afb1dd2e694a44fe07caaa14e3878db7fff54c514937611757d1a1bc2c6
- 93015b567e5ba8266205fb1183a6a26a3b950b67fd1366639ae232206d972f77
- c9094685ae4851fd5a5b886b73c7b07efd9b47ea0bdae3f823d035cf1b3b9e48
- 1a773948b5f177ca2e4561213ba2edeb08d4eeb05bd24635a1e7a2cbcd377bdd
- 30efcdccc49589dc32e51f2f8fc269f45d5eb62dfafa3886f685cdd2214dd35f
- 3347cc0b67cd8ad857d8f24b18a4c66776b1da6dbaac9b8fa077bda8218c73ab
- 4d5d3f9967db0ed61f9e48de6bab3f5b0a9f30e58da52e8b0dd8601e908f4743
- 6e04b543db11048a0b57fe786c0c52441ded217252cd6564fc63ff84ee486f10
- 72d2536c7a849a18bee4c3b574873371f05e8fcbd31f2b922f3231dbdce3f632
- 79805092438a2e9b753b68a4cc97ad2107b68935f16903f38456e9b39e0ac3d3
- c57b363df437c5ee108e0be22d63d6e2e8dc417246e3b13b18f3562cec2c5073
- f82a842c7d83381049ee3b1f29e54c80e08da5ecbb27101629efc615eca9fb61
- fb307e61f4ba0a09a023250422038b885d6926e9aa2027bcf56914d7a6a2f76a
- 04b99b0b9a0e98d04478003c86bf4fa3d20c56313c716b62e7be74ae7b95bf70
- 0dc2ed3a68353261b09be0a93070ccfb23f48786be6ba548ed0f9c373befe110
- 1522a865e9d583c3581fc19cafef5a41a7c7d0f759aaead3364045f300202305

[5] Three random words - NCSC.GOV.UK

- 1d9d5cfc8ad162af6100cf3311f83608dab90bb8b3f41ccf9fc441718dd33970
- 33c1d451e3a186d8734b27319b80036976cca882a6c531ddde9ad814cf42ef93
- 42d504e5df2c5ab253c8cdc8dbd7332a0714789af1822946db74d8eb951da162
- 51925d36298a3d9ceac6067fdc1ba1f799ef5c53553be95d6827192df0700d80

LummaC2 Associated IP Addresses:

- 104[.]21[.]37[.]53
- 77[.]73[.]134[.]68
- 144[.]76[.]173[.]247
- 157[.]90[.]248[.]179

LummaC2 Associated Domains:

- gstatic-node[.]io
- solopodvip-my[.]xyz
- 18866-32530[.]bacloud[.]info
- traftech[.]pro

LummaC2 Associated URLs:

- hxxp[://]gapi-node[.]io/
- hxxp[://]glitchmoon[.]xyz/
- hxxp[://]balancelag[.]xyz/
- hxxp[://]coursenote[.]xyz/
- hxxp[://]quotamoney[.]xyz/
- hxxp[://]acexoss[.]xyz/
- hxxp[://]checkgoods[.]xyz/
- hxxp[://]coolvtf[.]xyz/
- hxxp[://]costexcise[.]xyz/
- hxxp[://]doorblu[.]xyz/
- hxxp[://]freeace[.]xyz/
- hxxp[://]woodcat[.]xyz/
- hxxp[://]fisholl[.]xyz/
- hxxp[://]frogswordsale[.]xyz/
- hxxp[://]gitarlessonfinger[.]xyz/
- hxxp[://]goldenwalstk[.]xyz/
- hxxp[://]marketsale[.]xyz/
- hxxp[://]netforyou[.]xyz/
- hxxp[://]singlesfree[.]xyz/
- hxxp[://]survviv[.]xyz/

Threat Landscape

In recent years, information stealing malware, such as LummaC2 Stealer, have become a prevalent infection vector. More specifically, LummaC2 Stealer is a 'Commodity' information stealer and, as such, data harvested by these malware variants are often sold within the illicit marketplace, whereby threat actors have the opportunity to purchase them[6]. The acquisition of the credentials by threat actors will ultimately lead to further targeting, inevitably resulting in the implementation of additional attack vectors, such as ransomware. Information stealer malware variants, such as LummaC2, will remain undetected within the target landscape and, as such, they possess the ability to execute covertly, without their presence being detected.

Threat Group

No attribution to specific threat actors or groups has been identified at the time of writing.

Mitre Methodologies

Execution

T1053 – Scheduled Task[7]
T1059.001 – Command and scripting interpreter: PowerShell[8]

Persistence

T1053 – Scheduled Task[9]
T1547.001 – Registry Run Keys / Startup Folder[10]
T1543.003 – Create or Modify System Process: Windows Service[11]

Privilege Escalation

T1053 – Scheduled Task[12]
T1547.001 – Registry Run Keys / Startup Folder[13]
T1543.003 – Create or Modify System Process: Windows Service[14]

Defence Evasion

T1112 – Modify Registry[15]
T1553.004 – Subvert Trust Controls: Install Root Certificate[16]
T1562.001 – Impair Defenses: Disable or Modify Tools[17]
T1564.001 – Hide Artifacts: Hidden Files and Directories[18]

[6] The Next Generation of Info Stealers • KELA Cyber Threat Intelligence
[7] Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®
[8] Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®
[9] Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®
[10] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[11] Create or Modify System Process: Windows Service, Sub-technique T1543.003 - Enterprise | MITRE ATT&CK®
[12] Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®
[13] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[14] Create or Modify System Process: Windows Service, Sub-technique T1543.003 - Enterprise | MITRE ATT&CK®
[15] https://attack.mitre.org/techniques/T1112/
[16] Subvert Trust Controls: Install Root Certificate, Sub-technique T1553.004 - Enterprise | MITRE ATT&CK®
[17] Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®
[18] Hide Artifacts: Hidden Files and Directories, Sub-technique T1564.001 - Enterprise | MITRE ATT&CK®

Credential Access

T1552.001 – Unsecured Credentials: Credentials In Files[19]

Discovery

T1012 – Query Registry[20]
T1082 – System Information Discovery[21]
T1120 – Peripheral Device Discovery[22]

Collection

T1005 – Data from Local System[23]

Command and Control

T1102 – Web Service[24]

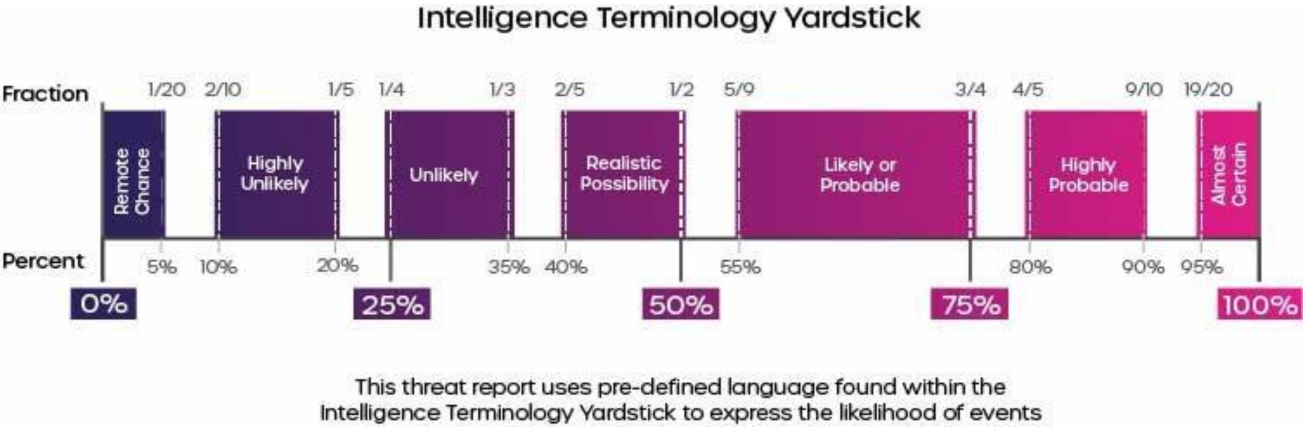
Impact

T1489 – Service Stop[25]
T1491 – Defacement[26]

Further Information

- SOC Radar Malware Analysis - LummaC2

Intelligence Cut-off Date (ICoD): 24/08/2023 10:00 UTC



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events

[19] Unsecured Credentials: Credentials In Files, Sub-technique T1552.001 - Enterprise | MITRE ATT&CK®
[20] Query Registry, Technique T1012 - Enterprise | MITRE ATT&CK®
[21] System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
[22] Peripheral Device Discovery, Technique T1120 - Enterprise | MITRE ATT&CK®
[23] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®
[24] Web Service, Technique T1102 - Enterprise | MITRE ATT&CK®
[25] Service Stop, Technique T1489 - Enterprise | MITRE ATT&CK®
[26] Defacement, Technique T1491 - Enterprise | MITRE ATT&CK®